UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

RICHARD WITAS, individually and on behalf of all others similarly situated, Plaintiff, v. INTRASYSTEMS, LLC and ALLEGHENY HEALTH NETWORK, Defendants.	**Case No.: 1:25-cv-10221** **COMPLAINT – CLASS ACTION** **JURY TRIAL DEMANDED**

Plaintiff Richard Witas ("Plaintiff"), on behalf of all others similarly situated, by and through his undersigned counsel, brings this Class Action Complaint against IntraSystems, LLC ("IntraSystems") and Allegheny Health Network ("AHN", and collectively "Defendants"). Plaintiff alleges the following upon information and belief based on and the investigation of counsel, except as to those allegations that specifically pertain to Plaintiff, which are alleged upon personal knowledge.

INTRODUCTION

1. Plaintiff and the proposed Class Members bring this class action lawsuit on behalf of all persons who entrusted Defendants with sensitive Personally Identifiable Information ("PII")[1] and Protected Health Information ("PHI") (collectively "Private Information") that was impacted in a data breach that Defendants publicly disclosed on January 17, 2025 (the "Data Breach" or the "Breach").

2. Plaintiff's claims arise from Defendants' failure to properly secure and safeguard Private Information that was entrusted to them, and their accompanying responsibility to store and transfer that information.

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual.

3. Defendant AHN is an integrated healthcare system based in Pittsburgh, Pennsylvania serving western Pennsylvania and surrounding regions. The network operates a wide range of hospitals, outpatient facilities, and medical practices across the area. Defendants offers specialized medical services in various fields, including oncology, cardiology, orthopedics, neurology, and women's health.[2]

4. Defendant IntraSystems is an IT consulting company, a managed services provider and systems integrator that specialized in the deployment and delivery of IT infrastructure, cybersecurity services and assessments, virtualization services, security and cloud solutions.[3]

5. As part of their operations, Defendants collect, maintain, and store highly sensitive Private Information belonging to AHN's patients.

6. Defendants had numerous statutory, regulatory, contractual, and common law duties and obligations, including those based on its affirmative representations to Plaintiff and Class Members, to keep their Private Information confidential, safe, secure, and protected from unauthorized disclosure or access.

7. On November 19, 2024, Defendants became aware of a security incident on their IT Network.[4] In response, Defendants launched an investigation and engaged third-party cybersecurity experts to determine the nature and scope of the incident.[5]

8. The investigation determined that unauthorized access occurred between October 11, 2024, and November 19, 2024, affecting patients who received services through AHN's home Medical Equipment and Home Infusion Therapy divisions.[6]

9. Defendants then launched a comprehensive review of the impacted data to determine what information was compromised and how many individuals were impacted.[7]

10. Upon information and belief, the following types of sensitive information may have been compromised in the data breach: names, addresses, date of birth, Social Security

[2] *About*, Allegheny Health Network: https://www.ahn.org/about (last visited January 28, 2025).
[3] *About us*, IntraSystems LLC: https://intrasystems.com/about-intrasystems/ (last visited January 28, 2025).
[4] *Exhibit 1*: Richard Witas Notice Letter.
[5] *Id.*
[6] *Id.*
[7] *Id.*

number, financial account numbers, health insurance information, treatment information, and medical device serial numbers.[8]

11. On January 17, 2025, AHN issued a notice with the Attorney General of Massachusetts and began sending notice letters to impacted individuals.[9]

12. Defendants failed to take precautions designed to keep their patients' Private Information secure.

13. Defendants owed Plaintiff and Class Members a duty to take all reasonable and necessary measures to keep the Private Information collected safe and secure from unauthorized access. Defendants solicited, collected, used, and derived a benefit from the Private Information, yet breached its duty by failing to implement or maintain adequate security practices.

14. Defendants admit that information in its system was accessed by unauthorized individuals, though it provided little information regarding how the Data Breach occurred.

15. The sensitive nature of the data exposed through the Data Breach signifies that Plaintiff and Class Members have suffered irreparable harm. Plaintiff and Class Members have lost the ability to control their private information and are subject to an increased risk of identity theft.

16. Defendants, despite having the financial wherewithal and personnel necessary to prevent the Data Breach, nevertheless failed to use reasonable security procedures and practice appropriate to the nature of the sensitive, unencrypted information it maintained for Plaintiff and Class Members, causing the exposure of Plaintiff's and Class Members' Private Information.

17. As a result of Defendants' inadequate digital security and notice process, Plaintiff's and Class Members' Private Information was exposed to criminals. Plaintiff and the Class Members have suffered and will continue to suffer injuries including: financial losses caused by misuse of their Private Information; the loss or diminished value of their Private

[8] *Id.*
[9] *Data Breach Notification*, Allegheny Health Network, OFFICE OF THE ATTORNEY GENERAL OF MASSACHUSETTS: https://www.mass.gov/doc/2025-97-allegheny-health-network/download (last visited January 28, 2025).

Information as a result of the Data Breach; lost time associated with detecting and preventing identity theft; and theft of personal and financial information.

18. Plaintiff brings this action on behalf of all persons whose Private Information was compromised as a result of Defendants failure to: (i) adequately protect the Private Information of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of Defendants inadequate information security practices; (iii) effectively secure hardware containing protected Private Information using reasonable and adequate security procedures free of vulnerabilities and incidents; and (iv) timely notify Plaintiff and Class Members of the Data Breach. Defendants conduct amounts to at least negligence and violates federal and state statutes.

19. Plaintiff brings this action individually and on behalf of a Nationwide Class of similarly situated individuals against Defendants for: negligence; negligence *per se*; unjust enrichment, breach of implied contract, and breach of confidence.

20. Plaintiff seeks to remedy these harms and prevent any future data compromise on behalf of himself and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and who remain at risk due to Defendants inadequate data security practices.

PARTIES

Plaintiff

21. Plaintiff Richard J Witas is a resident of Turtle Creek, Pennsylvania. On January 17, 2025, Defendants sent Plaintiff a notice letter informing him that his Private Information was compromised in the Data Breach. As a result of the Data Breach, Plaintiff has experienced an uptick in spam calls, emails, and text messages, and has been forced to, and will continue to, invest significant time monitoring his accounts to detect and reduce the consequences of likely identity fraud. As a result of the Data Breach, Plaintiff is now subject to substantial and imminent risk of future harm. Plaintiff would not have used Defendants services had he known that it would expose his sensitive Private Information.

Defendants

22. Defendant AHN is an integrated healthcare system based in Pittsburgh, Pennsylvania, having its principal place of business located at 120 Fifth Avenue, Suite 2900, Pittsburgh, Pennsylvania 15222.[10]

23. Defendant IntraSystems is an IT consulting company, managed services provider and systems integrator that specialized in the deployment and delivery of IT infrastructure, cybersecurity services and assessments, virtualization services, security and cloud solutions, headquartered in Braintree, Massachusetts, having its principal place of business located at 35 Braintree Hill Office Park, Suite 403, Braintree, Massachusetts 02184.[11]

JURISDICTION AND VENUE

24. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. The number of class members is more than 100 and at least one member of the Class defined below is a citizen of a different state that is diverse from Defendants' citizenship. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

25. This Court has jurisdiction over Defendants through their business operations in this District, the specific nature of which occurs in this District. IntraSystems' principal place of business is in this District. Defendants intentionally avail themselves of the markets within this District to render the exercise of jurisdiction by this Court just and proper.

26. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claims occurred in this District.

FACTUAL ALLEGATIONS

A. Background on Defendants

27. Defendant AHN is a medical system operating numerous hospitals, outpatient centers, cancer centers, surgery centers, urgent care offices, and other medical facilities in western Pennsylvania.[12]

---

[10] *Contact us,* Allegheny Health Network: https://www.ahn.org/about/contact-us (last visited January 28, 2025).
[11] *Contact us,* Intrasystems LLC: https://intrasystems.com/contact-us/ (last visited January 28, 2025).
[12] *About us*, Allegheny Health Network: https://www.ahn.org/about (last visited January 28, 2025).

28. Defendant IntraSystems is an IT software systems provider serving companies in numerous sectors, including the healthcare sector.[13]

29. As part of their operations, Defendants collect, maintain, and store highly sensitive Private Information belonging to AHN's patients.

30. Upon information and belief, Defendants made promises and representations to individuals, including Plaintiff and Class Members, that the Private Information collected from them would be kept safe and confidential, and that the privacy of that information would be maintained.[14][15]

31. Plaintiff and Class Members provided their Private Information to Defendants with the reasonable expectation and on the mutual understanding that Defendants would comply with their obligations to keep such information confidential and secure from unauthorized access.

32. As a result of collecting and storing the Private Information of Plaintiff and Class Members for their own financial benefit, Defendants had a continuous duty to adopt and employ reasonable measures to protect Plaintiff's and the Class Members' Private Information from access to third parties.

B. The Data Breach

33. On November 19, 2024, Defendants became aware of a security incident on their IT Network.[16] In response, Defendants launched an investigation and engaged third-party cybersecurity experts to determine the nature and scope of the incident.[17]

34. The investigation determined that unauthorized access occurred between October 11, 2024, and November 19, 2024, affecting patients who received services through AHN's Home Medical Equipment and Home Infusion Therapy divisions.

35. Defendants then launched a comprehensive review of the impacted data to determine what information was compromised and how many individuals were impacted.[18]

---

[13] *About us*, IntraSystems LLC: https://intrasystems.com/about-intrasystems/ (last visited January 28, 2025).
[14] *Privacy Policy,* Allegheny Health Network: https://www.ahn.org/about/privacy-policy (last visited January 28, 2025).
[15] *Privacy Policy*, IntraSystems, LLC: https://intrasystems.com/privacy-policy/ (last visited January 28, 2025).
[16] *Exhibit 1*: Richard Witas Notice Letter.
[17] *Id.*
[18] *Id.*

36. Upon information and belief, the following types of sensitive information may have been compromised in the data breach: names, addresses, date of birth, Social Security number, financial account numbers, health insurance information, treatment information, and medical device serial numbers.[19]

37. On January 17, 2025, AHN issued a notice with the Attorney General of Massachusetts and began sending notice letters to impacted individuals.[20]

38. Defendants failed to take precautions designed to keep individuals' Private Information secure.

39. While Defendants sought to minimize the damage caused by the Data Breach, it cannot and has not denied that there was unauthorized access to the sensitive Private Information of Plaintiff and Class Members.

40. Individuals affected by the Data Breach are, and remain, at risk that their data will be sold or listed on the dark web and, ultimately, illegally used in the future.

C. Defendants Failure to Prevent, Identify, and Timely Report the Data Breach

41. Defendants admit that an unauthorized third party accessed their IT Network. Defendants failed to take adequate measures to protect their computer systems against unauthorized access.

42. The Private Information that Defendants allowed to be exposed in the Data Breach is the type of private information that Defendants knew or should have known would be the target of cyberattacks.

43. Despite their own knowledge of the inherent risks of cyberattacks, and notwithstanding the FTC's data security principles and practices,[21] Defendants failed to disclose that their systems and security practices were inadequate to reasonably safeguard their past and present patients Private Information.

---

[19] *Id.*

[20] *Data Breach Notification*, Allegheny Health Network, OFFICE OF THE ATTORNEY GENERAL OF MASSACHUSETTS: https://www.mass.gov/doc/2025-97-allegheny-health-network/download (last visited January 28, 2025).

[21] *Protecting Personal Information: A Guide for Business,* FED. TRADE COMM'N (Oct. 2016), https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business. (last visited January 28, 2025).

44. The FTC directs businesses to use an intrusion detection system to expose a breach as soon as it occurs, monitor activity for attempted hacks, and have an immediate response plan if a breach occurs.[22] Immediate notification of a Data Breach is critical so that those impacted can take measures to protect themselves.

45. Here, Defendants waited for almost two months after being made aware of the Data Breach to notify impacted individuals.

D. The Harm Caused by the Data Breach Now and Going Forward

46. Victims of data breaches are susceptible to becoming victims of identity theft. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 17 C.F.R. § 248.201(9). When "identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance."[23]

47. The type of data that may have been accessed and compromised here can be used to perpetrate fraud and identity theft.

48. Plaintiff and Class Members face a substantial risk of identity theft given that their Private Information was compromised in the Data Breach.

49. Stolen Private Information is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines. Law enforcement has difficulty policing the "dark web" due to this encryption, which allows users and criminals to conceal their identities and online activity.

50. When malicious actors infiltrate companies and copy and exfiltrate the Private Information that those companies store, the stolen information often ends up on the dark web where malicious actors buy and sell that information for profit.[24]

---

[22] *Id.*

[23] *Prevention and Preparedness*, New York State Police, https://troopers.ny.gov/prevention-and-preparedness (last visited January 28, 2025).

[24] *Shining a Light on the Dark Web with Identity Monitoring*, IdentityForce (Dec. 28, 2020) https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring (last visited January 28, 2025).

51. For example, when the U.S. Department of Justice announced their seizure of AlphaBay—the largest online "dark market"—in 2017, AlphaBay had more than 350,000 listings, many of which concerned stolen or fraudulent documents that could be used to assume another person's identity."[25] Marketplaces similar to the now-defunct AlphaBay continue to be "awash with [PII] belonging to victims from countries all over the world."[26]

52. PII remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[27] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[28]

53. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses in 2019, resulting in more than $3.5 billion in losses to individuals and business victims.[29]

54. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[30] Defendants did not rapidly report to Plaintiff and Class Members that their Private Information had been stolen. Defendants notified impacted people after almost two months after learning of the Data Breach.

55. As a result of the Data Breach, the Private Information of Plaintiff and Class Members has been exposed to criminals for misuse. The injuries suffered by Plaintiff and Class Members, or likely to be suffered as a direct result of Defendants Data Breach, include: (a) theft of their Private Information; (b) costs associated with the detection and prevention of identity

---

[25] *Stolen PII & Ramifications: Identity Theft and Fraud on the Dark Web*, ARMOR (April 3, 2018), https://res.armor.com/resources/blog/stolen-pii-ramifications-identity-theft-fraud-dark-web/ (last visited January 28, 2025).
[26] *Id.*
[27] *Id.*
[28] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015) https://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited January 28, 2025).
[29] *2019 Internet Crime Report Released*, FBI (Feb. 11, 2020) https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120#:~:text=IC3%20received%20467%2C361%20complaints%20in,%2Ddelivery%20scams%2C%20and%20extortion (last visited January 28, 2025).
[30] *Id.*

theft; (c) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the consequences of this Breach; (d) invasion of privacy; (e) the emotional distress, stress, nuisance, and annoyance of responding to, and resulting from, the Data Breach; (f) the actual and/or imminent injury arising from actual and/or potential fraud and identity theft resulting from their personal data being placed in the hands of the ill-intentioned hackers and/or criminals; (g) damage to and diminution in value of their personal data entrusted to Defendants with the mutual understanding that Defendants would safeguard their Private Information against theft and not allow access to and misuse of their personal data by any unauthorized third party; and (h) the continued risk to their Private Information, which remains in the possession of Defendants, and which is subject to further injurious breaches so long as Defendants fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information.

56. In addition to a remedy for economic harm, Plaintiff and Class Members maintain an interest in ensuring that their Private Information is secure, remains secure, and is not subject to further misappropriation and theft.

57. Defendants disregarded the rights of Plaintiff and Class Members by (a) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that their network servers were protected against unauthorized intrusions; (b) failing to disclose that it did not have adequately robust security protocols and training practices in place to safeguard Plaintiff's and Class Members' Private Information; (c) failing to take standard and reasonably available steps to prevent the Data Breach; (d) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (e) failing to provide Plaintiff and Class Members prompt and accurate notice of the Data Breach.

58. The actual and adverse effects to Plaintiff and Class Members, including the imminent, immediate, and continuing increased risk of harm for identity theft, identity fraud and/or medical fraud directly or proximately caused by Defendants wrongful actions and/or inaction and the resulting Data Breach require Plaintiff and Class Members to take affirmative acts to recover their peace of mind and personal security including, without limitation, purchasing

credit reporting services, purchasing credit monitoring and/or internet monitoring services, frequently obtaining, purchasing and reviewing credit reports, bank statements, and other similar information, instituting and/or removing credit freezes and/or closing or modifying financial accounts, for which there is a financial and temporal cost. Plaintiff and other Class Members have suffered, and will continue to suffer, such damages for the foreseeable future.

CLASS ALLEGATIONS

59. Plaintiff brings this class action, individually and on behalf of the following Nationwide Class:

> All persons in the United States who were impacted by the Data Breach publicly announced by Defendants in January 2025 (the "Class").

60. Specifically excluded from the Class are Defendants, their officers, directors, agents, trustees, parents, children, corporations, trusts, representatives, principals, servants, partners, joint venturers, or entities controlled by Defendants, and their heirs, successors, assigns, or other persons or entities related to or affiliated with Defendants and/or their officers and/or directors, the judge assigned to this action, and any member of the judge's immediate family.

61. Plaintiff reserves the right to amend the Class definitions above if further investigation and/or discovery reveals that the Class should be expanded, narrowed, divided into subclasses, or otherwise modified in any way.

62. This action may be certified as a class action because it satisfies the numerosity, commonality, typicality, adequacy, and superiority requirements therein.

63. Numerosity: The Class is so numerous that joinder of all Class Members is impracticable. Although the precise number of such persons is unknown, and the facts are presently within the sole knowledge of Defendants, upon information and belief, Plaintiff estimates that the Class is comprised of thousands of Class Members, if not more. The Class is sufficiently numerous to warrant certification.

64. Typicality of Claims: Plaintiff's claims are typical of those of other Class Members because Plaintiff, like the unnamed Class, had his Private Information compromised as a result of the Data Breach. Plaintiff is a member of the Class, and his claims are typical of the claims of the

members of the Class. The harm suffered by Plaintiff is similar to that suffered by all other Class Members which was caused by the same misconduct by Defendants.

65. Adequacy of Representation: Plaintiff will fairly and adequately represent and protect the interests of the Class. Plaintiff has no interests antagonistic to, nor in conflict with, the Class. Plaintiff has retained competent counsel who are experienced in consumer and commercial class action litigation and who will prosecute this action vigorously.

66. Superiority: A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Because the monetary damages suffered by individual Class Members are relatively small, the expense and burden of individual litigation make it impossible for individual Class Members to seek redress for the wrongful conduct asserted herein. If Class treatment of these claims is not available, Defendants will likely continue their wrongful conduct, will unjustly retain improperly obtained revenues, or will otherwise escape liability for their wrongdoing as asserted herein.

67. Predominant Common Questions: The claims of all Class Members present common questions of law or fact, which predominate over any questions affecting only individual Class Members, including:

a. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

b. Whether Defendants data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

c. Whether Defendants storage of Plaintiff's and Class Member's Private Information was done in a negligent manner;

d. Whether Defendants had a duty to protect and safeguard Plaintiff's and Class Members' Private Information;

e. Whether Defendants conduct was negligent;

f. Whether Defendants conduct violated Plaintiff's and Class Members' privacy;

g. Whether Defendants conduct violated the statutes as set forth herein;

h. Whether Defendants took sufficient steps to secure their past and present patients Private Information;

i. Whether Defendants was unjustly enriched; and

j. The nature of relief, including damages and equitable relief, to which Plaintiff and Class Members are entitled.

68. Information concerning Defendants' policies is available from Defendants records.

69. Plaintiff knows of no difficulty which will be encountered in the management of this litigation which would preclude their maintenance as a class action.

70. The prosecution of separate actions by individual members of the Class would run the risk of inconsistent or varying adjudications and establish incompatible standards of conduct for Defendants. Prosecution as a class action will eliminate the possibility of repetitious and inefficient litigation.

71. Given that Defendants had not indicated any changes to their conduct or security measures, monetary damages are insufficient and there is no complete and adequate remedy at law.

CAUSES OF ACTION
COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

72. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above in paragraphs 1 through 20 and paragraphs 27 through 58 as though fully set forth herein.

73. Plaintiff brings this claim individually and on behalf of the Class Members.

74. Defendants knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

75. Defendants had a duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiff's and Class Members' Private Information.

76. Defendants had, and continues to have, a duty to timely disclose that Plaintiff's and Class Members' Private Information within their possession was compromised and precisely the types of information that were compromised.

77. Defendants owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards, applicable standards of care from statutory authority like Section 5 of the FTC Act, and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected individuals' Private Information.

78. Defendants' duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendants and their patients. Defendants were in a position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Plaintiff and Class Members from a data breach.

79. Defendants' duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendants is bound by industry standards to protect confidential Private Information.

80. Defendants breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' Private Information.

81. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff's and Class Members' Private Information;

b. Failing to adequately monitor the security of their networks and systems; and

c. Failing to periodically ensure that their computer systems and networks had plans in place to maintain reasonable data security safeguards.

82. Defendants, through their actions and/or omissions, unlawfully breached their duties to Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' Private Information within Defendants' possession.

83. Defendants, through their actions and/or omissions, unlawfully breached their duties to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiff's and Class Members' Private Information.

84. Defendants, through their actions and/or omissions, unlawfully breached their duty to timely disclose to Plaintiff and Class Members that the Private Information within Defendants possession might have been compromised and precisely the type of information compromised.

85. Defendants breached the duties set forth in 15 U.S.C. § 45, the FTC guidelines, the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity, and other industry guidelines. In violation of 15 U.S.C. § 45, Defendants failed to implement proper data security procedures to adequately and reasonably protect Plaintiff's and Class Members' Private Information. In violation of the FTC guidelines, *inter alia,* Defendants did not protect the Private Information it keeps; failed to properly dispose of personal information that was no longer needed; failed to encrypt information stored on computer networks; lacked the requisite understanding of their networks' vulnerabilities; and failed to implement policies to correct security issues.

86. It was foreseeable that Defendants' failure to use reasonable measures to protect Plaintiff's and Class Members' Private Information would result in injury to Plaintiff and Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches.

87. It was foreseeable that the failure to adequately safeguard Plaintiff's and Class Members' Private Information would result in injuries to Plaintiff and Class Members.

88. Defendants breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' Private Information to be compromised.

89. But for Defendants' negligent conduct and breach of the above-described duties owed to Plaintiff and Class Members, their Private Information would not have been compromised.

90. As a result of Defendants' failure to timely notify Plaintiff and Class Members that their Private Information had been compromised, Plaintiff and Class Members are unable to take the necessary precautions to mitigate damages by preventing future fraud.

91. As a result of Defendants negligence and breach of duties, Plaintiff and Class Members are in danger of imminent harm in that their Private Information, which is still in the

possession of third parties, will be used for fraudulent purposes, and Plaintiff and Class Members have and will suffer damages including: a substantial increase in the likelihood of identity theft; the compromise, publication, and theft of their personal information; loss of time and costs associated with the prevention, detection, and recovery from unauthorized use of their personal information; the continued risk to their personal information; future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the personal information compromised as a result of the Data Breach; and overpayment for the services or products that were received without adequate data security.

COUNT II
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Class)

92. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above in paragraphs 1 through 20 and paragraphs 27 through 58 as though fully set forth herein.

93. Section 5 of the FTC Act, 15 U.S.C. 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by Defendants of failing to use reasonable measures to protect Plaintiff's and Class Members' Private Information. Various FTC publications and orders also form the basis of Defendants' duty.

94. Defendants violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Plaintiff's and Class Members' Private Information and by failing to comply with industry standards.

95. Defendants' conduct was particularly unreasonable given the nature and amount of Private Information obtained and stored and the foreseeable consequences of a data breach on Defendants systems.

96. Class Members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes) were intended to protect.

97. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement

actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and Class Members.

98. As a result of Defendants negligence *per se*, Plaintiff and Class Members have been harmed and have suffered damages including, but not limited to: damages arising from identity theft and fraud; out-of-pocket expenses associated with procuring identity protection and restoration services; increased risk of future identity theft and fraud, and the costs associated therewith; and time spent monitoring, addressing, and correcting the current and future consequences of the Data Breach.

COUNT III
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

99. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above in paragraphs 1 through 20 and paragraphs 27 through 58 as though fully set forth herein.

100. Plaintiff and Class Members conferred a benefit upon Defendants by providing Defendants with their Private Information.

101. Defendants appreciated or had knowledge of the benefits conferred upon themselves by Plaintiff. Defendants also benefited from the receipt of Plaintiff's and Class Members' Private Information.

102. Under principles of equity and good conscience, Defendants should not be permitted to retain the full value of Plaintiff's and the Class Members' Private Information because Defendants failed to adequately protect their Private Information. Plaintiff and the proposed Class would not have provided their Private Information to Defendants had they known Defendants would not adequately protect their Private Information.

103. Defendants should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds received by it because of their misconduct and the Data Breach they caused.

COUNT IV
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)

104. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above in paragraphs 1 through 20 and paragraphs 27 through 58 as though fully set forth herein.

105. Plaintiff and the Class provided and entrusted their Private Information to Defendants. Plaintiff and the Class provided their Private Information to Defendants as part of Defendants regular business practices.

106. In so doing, Plaintiff and the Class entered into implied contracts with Defendants by which Defendants agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen, in return for the business services provided by Defendants. Implied in these exchanges was a promise by Defendants to ensure that the Private Information of Plaintiff and Class Members in their possession was secure.

107. Pursuant to these implied contracts, Plaintiff and Class Members provided Defendants with their Private Information. In exchange, Defendants agreed to, among other things, and Plaintiff and the Class understood that Defendants would: (1) provide services to Plaintiff sand Class Members'; (2) take reasonable measures to protect the security and confidentiality of Plaintiff and Class Members' Private Information; and (3) protect Plaintiff and Class Members' Private Information in compliance with federal and state laws and regulations and industry standards.

108. Implied in these exchanges was a promise by Defendants to ensure the Private Information of Plaintiff and Class Members in the possession was only used to provide the agreed-upon reasons, and that Defendants would take adequate measures to protect Plaintiff and Class Members' Private Information.

109. A material term of this contract is a covenant by Defendants that they would take reasonable efforts to safeguard that information. Defendants breached this covenant by allowing Plaintiff and Class Members' Private Information to be accessed in the Data Breach.

110. Indeed, implicit in the agreement between Defendants and Plaintiff and Class Members was the obligation that both parties would maintain information confidentially and securely.

111. These exchanges constituted an agreement and meeting of the minds between the parties.

112. When the parties entered into an agreement, mutual assent occurred. Plaintiff and Class Members would not have disclosed their Private Information to Defendants but for the prospect of utilizing Defendants' services. Conversely, Defendants presumably would not have taken Plaintiff and Class Members' Private Information if they did not intend to provide Plaintiff and Class Members with their services.

113. Defendants were therefore required to reasonably safeguard and protect the Private Information of Plaintiff and Class Members from unauthorized disclosure and use.

114. Plaintiff and Class Members would not have entrusted their Private Information to Defendants in the absence of their implied contracts with Defendants and would have instead retained the opportunity to control their Private Information.

115. Defendants breached the implied contracts with Plaintiff and Class Members by failing to reasonably safeguard and protect Plaintiff and Class Members' Private Information.

116. Defendants' failure to implement adequate measures to protect the Private Information of Plaintiff and Class Members violated the purpose of the agreement between the parties.

117. As a proximate and direct result of Defendants breaches of their implied contracts with Plaintiff and Class Members, Plaintiff and the Class Members suffered damages as described in detail above.

COUNT V
BREACH OF CONFIDENCE
(On Behalf of Plaintiff and the Class)

118. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above in paragraphs 1 through 20 and paragraphs 27 through 58 as though fully set forth herein.

119. At all times during Plaintiff's and Class Members' interactions with Defendants, Defendants was fully aware of the confidential and sensitive nature of Plaintiff's and Class Members' Private Information that Plaintiff and Class Members entrusted to Defendants.

120. As alleged herein and above, Defendants' relationship with Plaintiff and the Class was governed by terms and expectations that Plaintiff's and the Class Members' Private Information would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

121. Plaintiff and the Class entrusted Defendants with their Private Information with the explicit and implicit understandings that Defendants would protect and not permit the Private Information to be disseminated to any unauthorized third parties.

122. Plaintiff and the Class also entrusted Defendants with their Private Information with the explicit and implicit understandings that Defendants would take precautions to protect that Private Information from unauthorized disclosure.

123. Defendants voluntarily received Plaintiff's and Class Members' Private Information in confidence with the understanding that their Private Information would not be disclosed or disseminated to the public or any unauthorized third parties.

124. As a result of Defendants' failure to prevent and avoid the Data Breach from occurring, Plaintiff's and Class Members' Private Information was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and Class Members' confidence, and without their express permission.

125. As a direct and proximate cause of Defendants actions and omissions, Plaintiff and the Class have suffered damages.

126. But for Defendants disclosure of Plaintiff's and Class Members' Private Information in violation of the parties' understanding of confidence, their Private Information would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendants Data Breach was the direct and legal cause of the theft of Plaintiff's and Class Members' Private Information as well as the resulting damages.

127. The injury and harm Plaintiff and the Class suffered was the reasonably foreseeable result of Defendants unauthorized disclosure of Plaintiff's and Class Members' Private Information. Defendants knew or should have known their methods of accepting and securing Plaintiff's and Class Members' Private Information was inadequate as it relates to, at the very least, securing servers and other equipment containing Plaintiff's and Class Members' Private Information.

128. As a direct and proximate result of Defendants breach of their confidence with Plaintiff and the Class, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) identity theft; (ii) the loss of the opportunity how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual present and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their Private Information, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information of current and former people; and (viii) present and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact

of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

129. As a direct and proximate result of Defendants' breaches of confidence, Plaintiff and the Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, seeks judgment against Defendants, as follows:

(a) For an order determining that this action is properly brought as a class action and certifying Plaintiff as the representative of the Class and his counsel as Class Counsel;

(b) For an order declaring that Defendants' conduct violates the laws referenced herein;

(c) For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

(d) For damages in amounts to be determined by the Court and/or jury;

(e) For an award of statutory damages or penalties to the extent available;

(f) For pre-judgment interest on all amounts awarded;

(g) For an order of restitution and all other forms of monetary relief; and

(h) Such other and further relief as the Court deems necessary and appropriate.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

[SIGNATURE BLOCK ON FOLLOWING PAGE]

Dated: January 28, 2025

By: /s/ *Gary Ishimoto*
Gary Ishimoto
Mark Svensson*
LEVI & KORSINSKY, LLP
33 Whitehall Street, 17th Floor
New York, NY 10004
Telephone: (212) 363-7500
Facsimile: (212) 363-7171
Email: gishimoto@zlk.com
Email: msvensson@zlk.com

Attorneys for Plaintiff and the Proposed Class

**pro hac vice* forthcoming